AKE in Clustered Ad Hoc Networks

Maarit Hietalahti
Helsinki University of Technology
Laboratory for Theoretical Computer Science
Maarit.Hietalahti@hut.fi

T-79.7001 Postgraduate Course in Theoretical Computer Science. 1.12.2006

Ad hoc networks

- what it is, what it isn’t?
- wireless and mobile
- usually radio connections
- self-organized network, where the user need not concern herself with network management

Clusters and hierarchy

- A cluster is a collection of nodes (geometrically) close together
- Clusters can be formed for a common cause or as a reaction to a factor that is common to the nodes
- A cluster-head is a special node in a cluster that acts as a leader for the cluster. Not always necessary
- A hierarchical structure in a network is composed of nested groupings (clusterings) of nodes
- Hierarchical routing: A route from a leaf node to another is formed via the routes between their respective groups
- Hybrid systems: intra-cluster and intercluster methods are different
- A *two-tier ad hoc network* means a hierarchical network consisting of only two layers

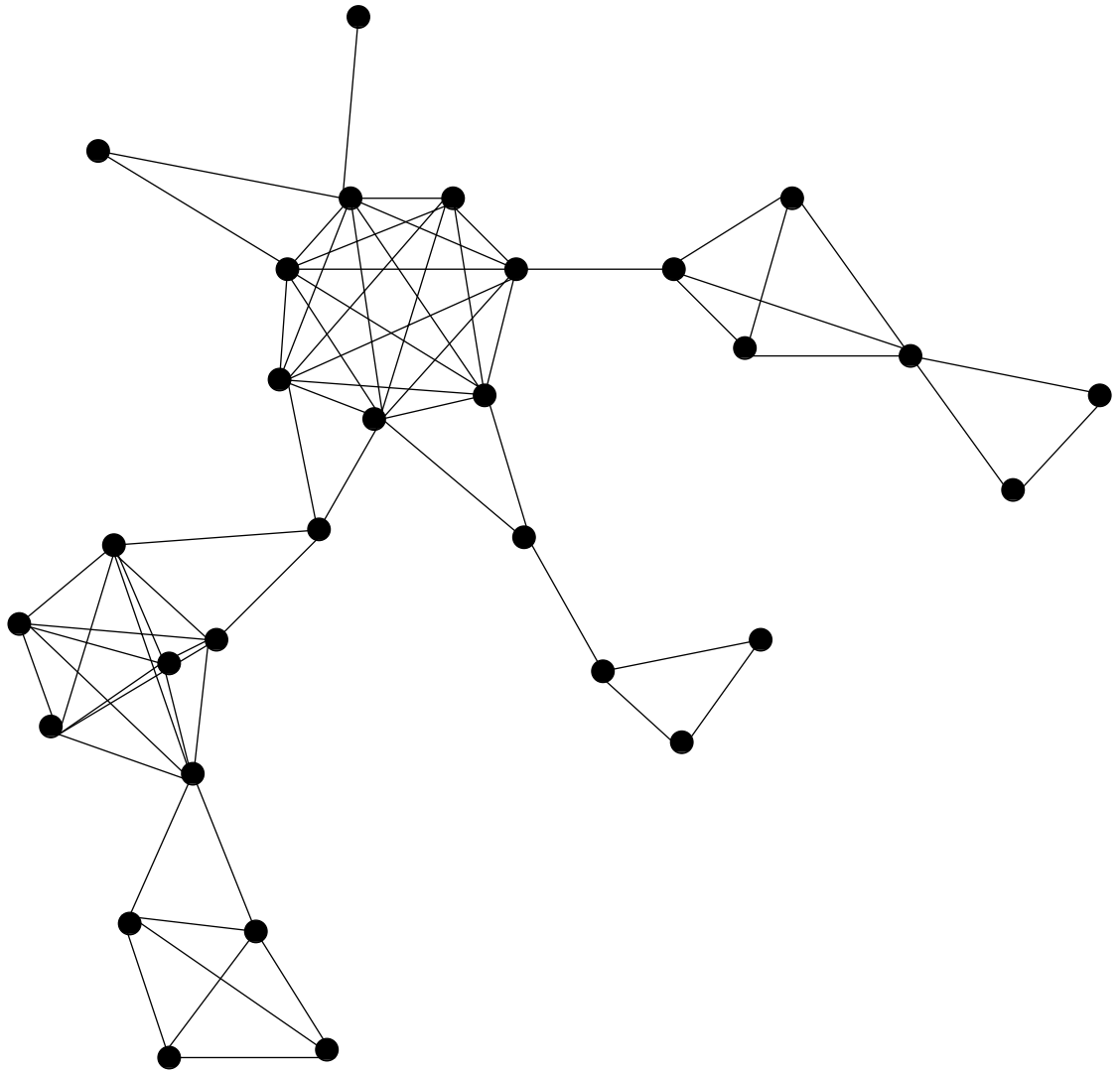

Figure 1: An example network

Clusterings

- Clustering algorithms differ in what types of clusters they produce
- Cluster-heads: for cluster formation and/or cluster maintenance
- Some clustering algorithms form cliques, i.e., clusters where every node is at a one hop distance from every other node [KVCP97]
- Some only require that the distance to the cluster-head is one hop
- The clusters are assumed to stay together longer than the nodes do in average.
- More stable internal connections due to the greater amount of links between nodes in a same cluster
- If there is a common background, they are likely to have a lot of internal communications as well

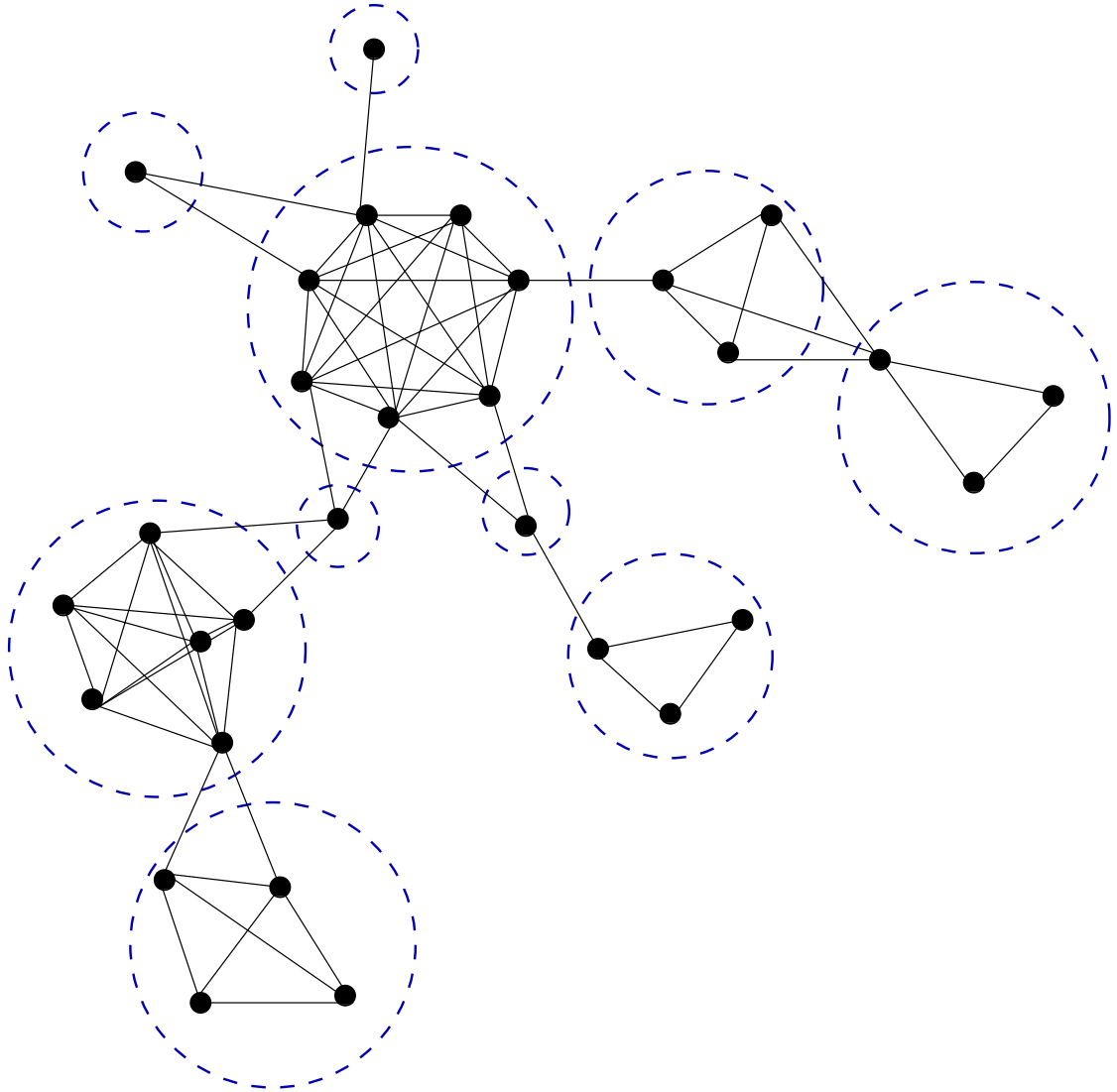

Figure 2: An example: non-overlapping clustering

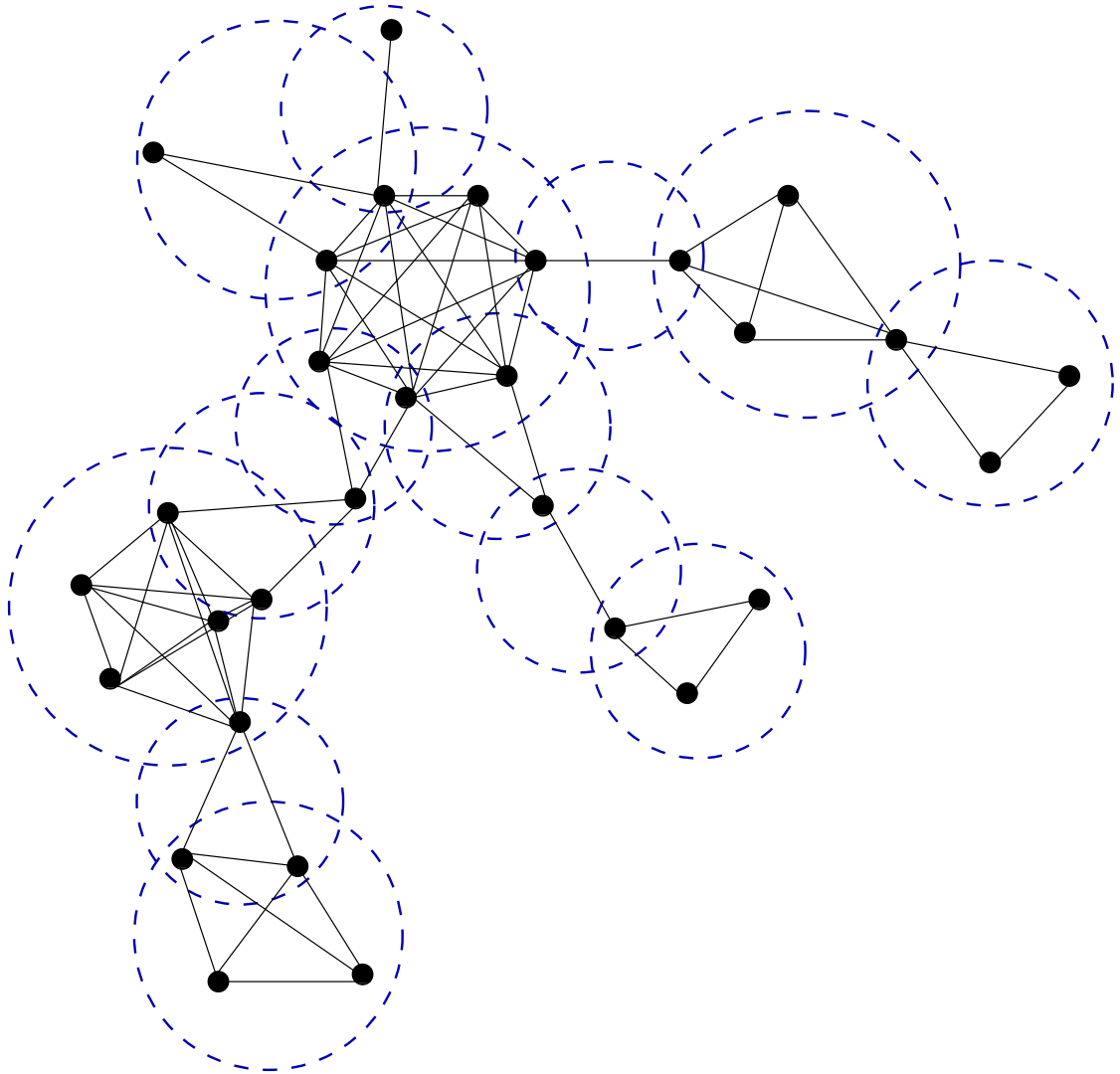

Figure 3: An example: overlapping clustering

Group keys

- a common symmetric key for a group of two or more participants
- For two participants, the *Diffie-Hellman key exchange* is often the most convenient choice. The multi-party case requires a generalization of a two-way key exchange
- *distributory* and *contributory* group key protocols

Broadcast protocol

This protocol was presented by Burmester and Desmedt [BD94]. It assumes that every node is at a one hop distance from another. The protocol is accomplished with only two broadcasts.

G is a finite cyclic group and g is a generator of G.

1. Each node m_i selects a random exponent r_i and broadcasts $z_i = g^{r_i}$ 2. Each node m_i computes and broadcasts $x_i = (z_{i+1}/z_{i-1}1)^{r_i}$ 3. Each node computes the session key $k_i = z_{i-1}^{nr_i} x_i^{n-1} x_{i+1}^{n-2} \cdots x_{i+n-2}$

TGDH [KPT00]

- Uses Diffie-Hellman key exchange in binary key trees
- The described structure of the results from the dynamic group key operations:join, leave, merge and partition
- There is no initial key agreement protocol: difficult to compare

AT-GDH

- The operations propagate over the network along the spanning tree
- All leaf nodes (nodes with no children) start:
- Selecting a random secret exponent e_{leaf} and blind it by calculating $f(e_{leaf}) = \alpha^{e_{leaf}}$ and send the result to their respective parents.
- After a node has received the blinded keys from all its children, they select their exponents e_{parent}
- Form Diffie-Hellman-type keys with their children repeatedly using the resulting key as the new exponent
- For example, the key formed with child one $k_1 = f(e_1)^{e_{parent}}$ is used as the parents new exponent: $k_{12} = f(e_2)^{k_1}$

AT-GDH continued

- The nodes do not send these keys to the children yet
- The secret formed with the last child serves as the node's new private key
- The node blinds the key and sends it to parents
- When parent has received similar messages from all its children, it can repeat the same computation
- This continues until the root has received all of its children's blinded keys
- The root repeats the same kind of computation as all the other parent nodes
- The secret key formed thus between the root and its last child (and all other nodes) will be the shared session key material for the entire network
- The blinded keys needed for extracting the group key are propagated up the tree from the parents to their children starting from the root

Ad hoc network environment

- global broadcast is most probably out of the question
- some occasions, a local broadcast from a node to its neighbors is feasible
- no fixed topology, such as a ring or a star can be assumed
- protocols requiring a specific topology either cannot be used at all or become inefficient
- initially no third parties that can be trusted to calculate a random key safely and to distribute it

Authenticated group key establishment

- Implicit key authentication means that a principal can be sure that no-one outside the group can learn the key without the help of a dishonest participant
- Key confirmation means that after the key has been established, the participants are assured that all legitimate participants do share the same key
- Explicit Key Authentication: implicit key authentication and key confirmation hold

Generic model: key establishment in clusters

- nodes form clusters
- key-tree (backbone) is formed from the clusters
- the initial key agreement begins
- subgraphs first, and then combined for a whole group wide key
- typically recursive Diffie-Hellman key exchange (bipartite or tripartite) also pairing-based
- a group key is constructed so that every node can calculate it using its own secret and the blinded secrets of others, or combinations of them

Example: Rhee et al. [RPT05]

- implicitly certified public keys (ICPK) [G8̈9], an ID-based public key scheme
- key confirmation message added to the key agreement protocol makes the protocol explicitly authenticated
- a two layered hierarchy is prompted by a physically two-layered network, ground nodes and unmanned aerial vehicles
- clusters of nodes below use a centralized system: distributed only
- aerial vehicles use TGDH

Example: ACEKA [SH06]

- ternary trees with the Joux tripartite Diffie-Hellman key agreement [Jou00]
- virtual backbone and virtual nodes in addition to the real nodes
- ACEKA uses clusterheads and “sponsors” for management
- authentication by signing every message using ID-based cryptography, with a variant of the ElGamal signature scheme

A new hybrid group key establishment

- A clustering mechanism that creates clusters where nodes are at a one hop distance from each other, i.e., cliques
- Then, the most efficient group key agreement protocol is the broadcast protocol by Burmester and Desmedt
- Two rounds of broadcasts (everyone broadcasts twice)
- each node can calculate the common group key from its own secret exponent and the blinded shares of others

A new hybrid group key establishment, continued

- clusters agree a group key by AT-GDH protocol
- clusterhead represents its cluster and use the cluster key as its secret exponent
- clusterheads distribute the needed key parts also in their cluster, so that other nodes can also calculate the network wide group key
- clusterheads are not necessarily at a one hop distance from each other, the messages need to be relayed by other members of the cluster (who know the secret already)
- relaying adds some extra links to the path

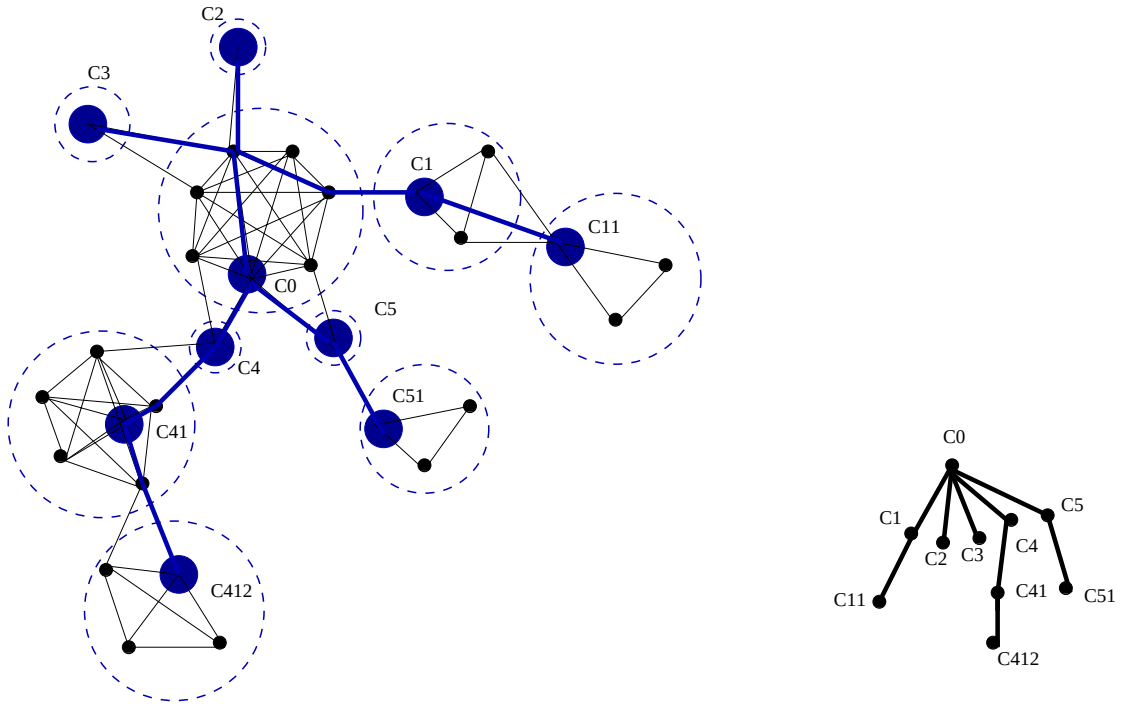

Figure 4: cluster-tree

Efficiency

- Radio connections can easily create large cliques, especially in homogeneous networks
- Theoretically, every clique forms a group key in two synchronous rounds, i.e., constant amount
- The amount of AT-GDH synchronous rounds is logarithmic to the number of participants
- In the end, clusterheads broadcast the key parts to clusters in one synch. round
- The resulting communication complexity (in theory) is logarithmic to the number of clusters

Adding authentication

- Previously group key agreements relied much on the implicit key authentication (A-GDH)
- Pereira and Quisquater [PQ04] showed that it is impossible to design a scalable authenticated group key agreement protocol on the same building blocks as A-GDH (dealt with previously in this seminar)
- Authentication with ID-based crypto, such as the ICPK public keys with key confirmation messages could be used with this protocol, as it is independent of the group key establishment method used

Conclusions

- Clustering can help also in group key establishment
- Some existing solutions for clustered group key establishment were surveyed
- New protocol: the cluster-based extension of AT-GDH combined to the broadcast group key protocol
- Efficient: the number of synchronous rounds: logarithmic to the number of clusters

Future work

- Maybe more efficient with tripartite key exchange realized with bilinear pairings as in [LKKR03]
- The form of the tree and clusters also affects the efficiency of the group key establishment. How much?
- Mobility: group key establishment is not always enough. –>
- Needs maintenance. At least the key should be updated when nodes join or leave the network, to preserve its contributory property. (Outside the scope of this paper)

References

[BD94] M. Burmester and Y. Desmedt. A secure and efficient conference key distribution system. In *Advances in Cryptology –Proceedings of EUROCRYPT*, volume 950 of *LNCS*, pages 275–286, Perugia, Italy, May 1994. Springer.

[G̈89] C. Günther. An identity–based key exchange protocol. In *Advances in Cryptology –Proceedings of EUROCRYPT*, volume 434 of *LNCS*, pages 29–37, 1989.

[Jou00] A. Joux. A one round protocol for tripartite Diffie–Hellman. In *Proceedings of Algorithmic Number Theory Symposium IV*, volume 1838 of *LNCS*, pages 385–394. Springer, 2000.

[KPT00] Y. Kim, A. Perrig, and G. Tsudik. Simple and fault–tolerant key agreement for dynamic collaborative groups. In *Proceedings of the Conference on Computer and Communications Security (CCS)*, pages 235–244, Athens, Greece, November 2000. ACM.

[KVCP97] P. Krishna, N. H. Vaidya, M. Chatterjee, and D. K. Pradhan. A cluster–based approach for routing in dynamic networks. *ACM SIGCOMM Computer Communication Review*, pages 49–65, April 1997.

[LKKR03] S. Lee, Y. Kim, K. Kim, and D. H. Ruy. An efficient tree–based group key agreement using bilinear map. In *Applied Cryptography and Network Security ACNS*, volume 2486 of *LNCS*, pages 357–371. Springer, 2003.

[PQ04] O. Pereira and J.-J. Quisquater. Generic insecurity of cliques-type authenticated group key agreement protocols. In *Proceedings of the Computer Security Foundations Workshop (CSFW)*. IEEE, June 2004.

[RPT05] K. H. Rhee, Y. H. Park, and G. Tsudik. A group key management architecture for mobile ad-hoc wireless networks. *Journal of Information Science and Engineering*, 21:415–428, 2005.

[SH06] H. Shi and M. He. Authenticated and communication efficient group key agreement for ad hoc networks. In *To appear at CANS '06*, December 2006.